CLAIMS

What is claimed is:

1. An agent process for controlling access to digital assets in a data processing environment comprising:

sensing atomic level asset access events, the sensing step located within an operating system kernel within a user client device;

aggregating multiple atomic level events to determine a combined event; and

asserting a policy violation predicate if a at least one combined event has occurred that violates a predefined digital asset usage policy.

2. A process as in Claim 1 wherein the step of asserting the policy violation predicate is implemented in an operating system kernel of the client user device.

3. A process as in Claim 1 additionally comprising:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy.

4. A process as in Claim 3 wherein the preventing step includes an IRP intercept.

5. A process as in Claim 1 wherein the combined event is a time sequence of multiple atomic level events.

6. A process as in Claim 1 additionally comprising:

prompting a user to document a reason for a policy violation, prior to granting access to the digital asset.

7. A process as in Claim 1 additionally comprising:

asserting multiple policy violation predicates such that any one predicate can veto the operation of other predicates.

8. A process as in Claim 2 that operates independently of application software.

9. A process as in Claim 1 additionally comprising:

notifying a user of a policy violation, and then permitting access to the digital asset.

10. A process as in Claim 2 wherein the sensors, aggregators, and asserting steps operate in real time.

11. A process as in Claim 1 additionally comprising:

determining the identity of a particular file in the asset access event.

12. A system for controlling access to digital assets in a data processing environment comprising:

an atomic level asset access event sensor, the sensor located within an operating system kernel within a user client device;

an atomic level event aggregator, to determine the occurrence of an aggregate event that comprises more than one atomic level asset access event; and

a policy violation detector, for determining if a combination of combined events have occurred that violates a predefined digital asset usage policy.

13. An apparatus as in Claim 12 wherein the policy violation detector is located in an operating system kernel of the user client device.

14. An apparatus as in Claim 12 wherein the policy violation detector determines a violated policy type.

15. An apparatus as in Claim 14 wherein the policy violation detector includes an IRP intercept.

16. An apparatus as in Claim 12 wherein the combined event is a time sequence of multiple atomic level events.

17. An apparatus as in Claim 12 wherein a user interface within the client device requires a user to document a reason for a policy violation prior to granting access to the digital asset.

18. As apparatus as in Claim 12 wherein the policy violation detector additionally asserts multiple policy violation predicates such that any one predicate can veto the operation of other predicates.

19. An apparatus as in Claim 13 that operates independently of application software.

20. An apparatus as in Claim 12 additionally comprising:

a user interface running on the user client device for notifying a user of a policy violation; and

permitting access to the digital asset once a reason for the violation is provided by the user.

21. An apparatus as in Claim 12 wherein the sensor, aggregator and detector operate in real time.

22. An apparatus as in Claim 12 wherein the detector additionally determines the identity of a particular file in the atomic level asset event.